REMARKS

The foregoing amendments and the following remarks are responsive to the Office Action mailed November 10, 2003. Applicants respectfully request reconsideration of the present application.

Claims 1-23 are pending. Claims 1, 20, and 23 have been amended. New claims 24-26 have been added. Therefore, claims 1-26 are presented for examination.

Examiner rejected claims 1-4 and 6-9 under 35 U.S.C. §102(e) as being unpatentable over U.S. Patent No. 5,534,855 issued to Shockley, et al. Examiner rejected claim 5 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,534,855 issued to Shockley, et al. and further in view of U.S. Patent No. 5,867,578 issued to Brickell, et al. Examiner rejected claims 13-21 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,534,855 issued to Shockley, et al. and further in view of U.S. Patent No. 6,587,946 issued Jakobsson.

Shockley discusses using biometrics for alias detection, i.e. to detect the actual identity of a user who may be using a different handle, or name, on a system. Shockley discusses that each user has an "account" or multiple accounts which "has a respective account identification to enable each individual user 10a-10c to log on to the computer system 10 and use a particular application identified in the name server system 18. This account of Shockley is a user account, identifying the user. Shockley states that the account is used for "storing in respective user accounts identification information uniquely characterizing each of a plurality of computer users." Shockley specifically states that "At no time during the authentication process is the CBAD data [certificate based alias detection data, which is integrity-locked digitized canonical biometric data] in the account certificate used." (Shockley, column 6, lines 44-46). Shockley further states that "Since CBAD data is not used to determine the validity of a remote delegation certificate, there is no compromise to the remote request authentication system if CBAD data is public.

(Shockley, column 7, lines 3-6). Thus, Shockley specifically teaches away from using biometric data (CBAD) for authentication, or to perform remote services. Shockley uses the CBAD data only for determining user distinctness and detecting alias accounts. (Shockley, column 7, lines 52-55).

In contrast, claim 1 of the present invention recites:

> A method of providing remote cryptographic services, the method comprising:
> a client requesting a cryptographic service;
> establishing a secure connection between the client and a biometric certification server (BCS);
> receiving biometric data from a user; and
> the BCS performing the cryptographic service if the user is authenticated based on the biometric authentication.

(Claim 1, as amended). As described above, Shockley specifically discusses using a digitally signed "login delegation certificate" via a smart card (Shockley, column 6, lines 31-37). Shockley does not teach or suggest performing a cryptographic service if a user is authenticated based on biometric authentication. The Examiner refers to column 6, lines 39-49 of Shockley which read:

> If the validation is successful, the operating system knows that the public key obtained from the account certificate matches the private key in the possession of the individual user trying to log on, and is justified in assigning to that individual user any rights or privileges associated with the account. At no time during the authentication process is the CBAD data in the account certificate used. Since CBAD data does not determine the success or failure of a login authentication, there is no compromise to the integrity of the login authentication system if CBAD data is public

(Shockley, column 6, lines 39-49). This portion of Shockley clearly teaches away, in that it states that at no time during the authentication process is the CBAD data used. The CBAD data is the only biometric data used by Shockley. Thus, contrary to Examiner's suggestion, this portion of Shockley teaches away from using the biometric data for validation. Therefore, claim 1 is not anticipated by, nor obvious over, Shockley. Claims 2-9 depend on claim 1, and incorporate its limitations, therefore they are not obvious or anticipated by Shockley for at least the same reasons advanced with respect to claim 1.

Claim 10 recites:

> A method of providing a certificate from a client to a server, the method comprising:
> receiving a request for a certificate from the server;
> forwarding the request to a biometric certification server (BCS);
> receiving a biometric identification from the client and forwarding the biometric identification to the BCS;
> if the biometric identification matches a registered user on the BCS, receiving a certificate including a public key of the client certified by the BCS; and
> forwarding the certificate to the server, thereby identifying the client to the server.

(Claim 10). The Examiner refers to column 11, line 49 to column 12, line 30 of Shockley. However, that portion of Shockley is concerned only with validating that a user is distinct from a previous user. Shockley does not teach or suggest a biometric certification server, as distinct from a server that is requesting data. Furthermore, Shockley does not teach or suggest receiving biometric identification from a client. Rather, Shockley uses the embedded CBAD data in a user's account certificate and compares it with the account certificate of an originator. No user provides a biometric identification in Shockley's system. Therefore, claim 10, and claims 11-12 which depend on it, are not anticipated by or obvious over Shockley.

Examiner rejected claim 5 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,534,855 issued to Shockley, et al. and further in view of U.S. Patent No. 5,867,578 issued to Brickell, et al. Brickell discusses a multi-step digital signature system, in which certifying authority members attach partial signatures to a message, and the combined set of partial signatures is used. Brickell does not teach or suggest a biometric certification server that provides cryptographic services on request, once a user is properly authenticated. Rather, Brickell only addresses a conventional certification server, which does not receive biometric data, nor does it provide "cryptographic services" but simply creates a digital certificate. Therefore, Brickell does not remedy the shortcomings of Shockley discussed above, and claim 5 is not obvious over Shockley in view of Brickell.

The Examiner rejected claims 13-21 under Shockley in view of Jacobsson. Jacobbson discusses a quorum controlled asymmetric proxy encryption. Asymmetric proxy encryption is sharing portions of a secret key among multiple proxy-servers.

Claim 13 recites:

> An apparatus for performing remote cryptographic functions comprising:
> a crypto-proxy interface for receiving a request for a cryptographic function from a client on a secure connection;
> an authentication engine for authenticating the user based on biometric data;
> a cryptographic engine for performing the cryptographic functions; and
> the crypto-proxy interface for returning data to the client, after the cryptographic functions are performed.

(Claim 13). As noted above, Shockley does not teach or suggest an authentication engine to authenticate a user based on biometric data, nor receiving a request for a cryptographic function from a client. Jacobbson does not teach or suggest receiving a request for a cryptographic function from a client, nor user authentication based on biometric data. Therefore, Jacobbson does not remedy the shortcomings of Shockley discussed above. And claim 13, and claims 14-21 which depend on it, are not obvious over Shockley in view of Jacobbson.

Examiner rejected claims 22 and 23 under 35 U.S.C. §102(e) as being unpatentable over U.S. Patent No. 6,507,912 issued to Matyas, Jr., et al.

Matyas discusses protection of biometric data using key-dependent sampling. The biometric data is sampled at a key-dependent sample frequency, and the key is applied to the biometric data. The key is a random number, a plurality of random numbers, or other values, which are used to set a sampling frequency or sampling parameters. However, Matyas does not teach or suggest using biometric data to permit a user to request a cryptographic function. Rather, Matyas uses conventional public key cryptography to protect a biometric key when it is sent to the user's system.

Claim 22, on the other hand, recites:

An apparatus for permitting remote cryptographic functions comprising:
a crypto-API (application program interface) for receiving cryptographic function requests; and
a cryptographic service provider for establishing a secure connection to a remote crypto-server, and having the crypto-server perform the cryptographic function; and
a sensor for receiving biometric data from a user, the biometric data sent to the crypto-server to authenticate the user, the remote crypto-server to perform the requested cryptographic function when the user is successfully authenticated using the biometric data

(Claim 22, as amended). Matyas does not teach or suggest a remote crypto-server to perform a requested cryptographic function. Rather, Matyas' system uses encryption to securely transmit biometric data (Matyas, column 4, line 48-51). Matyas does not teach or suggest a crypto-server that performs a requested cryptographic function. Therefore, claim 22, as amended, is not anticipated by or obvious over Matyas.

Claim 23 recites:

An apparatus comprising:
a client comprising:
a crypto-API (application program interface) for receiving cryptographic function requests; and
a cryptographic service provider for establishing a secure connection to a remote crypto-server, and having the crypto-server perform the cryptographic function; and
a sensor for receiving biometric data from a user, the biometric data sent to the crypto-server to authenticate the user;
the remote crypto-server comprising:
a crypto-proxy interface for receiving a request for the cryptographic function from the client on the secure connection;
an authentication engine for authenticating the user based on the biometric data;
a cryptographic engine for performing the requested cryptographic functions; and
the crypto-proxy interface for returning data to the client, after the cryptographic functions are performed.

Matyas does not teach or suggest a cryptographic engine for performing the requested cryptographic functions. The server of Matyas is designed for biometric authentication only. Matyas does not teach or suggest cryptographic functions, requested

by the user, performed by a crypto-server. Therefore, claim 23 is not anticipated by or obvious over Matyas.

In view of the foregoing amendments and remarks, applicants respectfully submit that all pending claims are in condition for allowance. Such allowance is respectfully requested.

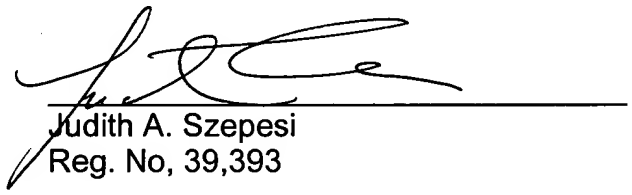
If the Examiner finds any remaining impediment to the prompt allowance of these claims that could be clarified with a telephone conference, the Examiner is respectfully requested to contact Judith A. Szepesi at (408) 720-8300.

If there are any additional charges, please charge Deposit Account No. 02-2666.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Date: 4/12 2004



Judith A. Szepesi
Reg. No, 39,393

12400 Wilshire Blvd.
Seventh Floor
Los Angeles, CA 90025
(408) 720-8300